UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/750,967	12/28/2000	Robert Watson	002.0165.01	7757

22895 7590 05/26/2004

PATRICK J S INOUYE P S
810 3RD AVENUE
SUITE 258
SEATTLE, WA 98104

EXAMINER	
CHANG, JUNGWON	
ART UNIT	**PAPER NUMBER**
2154	4

DATE MAILED: 05/26/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/750,967	Applicant(s) WATSON ET AL.	
	Examiner Jungwon Chang	Art Unit 2154	

– The MAILING DATE of this communication appears on the cover sheet with the correspondence address –

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 May 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are presented for examination.

2. The cross reference related to the application cited in the specification must be updated (i.e., update the relevant status with PTO Serial Number or patent number where appropriate on page 14, lines 17-20; and page 16, line 29 – page 17, line 2).

3. This Office action has an attached requirement for information under 37 C.F.R. § 1.105. A complete response to this Office action must include a complete response to the attached requirement for information. The time period for reply to the attached requirement coincides with the time period for reply to this Office action.

In response to this requirement, please provide a copy of each of the following items of art referred to in the specification on page 2, lines 16-19, page 8, lines 25-28, page 10, lines 1-4, page 11, lines 20-23.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-12 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

a. The following terms lack proper antecedent basis:

i. the requested server – claim 1, line 10; claim 7, line 8;

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Craig A. Huegen "The Latest in Denial of Service Attacks: "Smurfing" Description and Information to Minimize Effects", 2/8/2000, in view of CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks, Sep. 19, 1996 (Last Revised: Nov. 29, 2000), hereinafter CERT.

8. As to claims 1 and 7, Huegen discloses the invention as claimed, including a method for negotiating multi-path connections between a plurality of intermediary devices (i.e., router, broadcast device) (page 1, last paragraph; page 2, last paragraph to page 3, first paragraph; page 6, INFORMATION FOR VICTIMS AND HOW TO

SUPPRESS ATTACKS, paragraphs 3-6, i.e., Cisco routers have several "paths" which packets can take to be routed) in a networked computing environment, comprising:

establishing a client-side connection between a requesting client (i.e., attacker) and an intermediary device (i.e., router, broadcast device) (page 1, DESCRIPTION, lines 1-4; page 2, HOW TO KEEP YOUR SITE FROM BEING THE SOURCE PERPETRATORS USE TO ATTACK VICTIMS, lines 1-3) available from a plurality of intermediary devices on a primary communications channel (i.e., IP network; page 1, DESCRIPTION) in accordance with a connection-oriented network protocol (i.e., Transmission Control Protocol (TCP), User Datagram Protocol (UDP); page 9, OTHER DENIAL OF SERVICE ATTACKS WORTHY OF MENTION);

establishing a server-side connection between the intermediary device (i.e., router, broadcast device) and the requested server (i.e., spoofed address target, or victim host; page 1, DESCRIPTION, lines 5-10) on a primary communications channel (i.e., IP network; page 1, DESCRIPTION) in accordance with the connection-oriented network protocol (i.e., Transmission Control Protocol (TCP), User Datagram Protocol (UDP); page 9, OTHER DENIAL OF SERVICE ATTACKS WORTHY OF MENTION);

determining differences in connection parameters defined for the client-side connection and the server-side connection (i.e., differences between routing parameters used in client-side and server-side; page 2, HOW TO KEEP YOUR SITE FROM BEING THE SOURCE PERPETRATORS USE TO ATTACK VICTIMS, paragraph 4, i.e., checking the source address of a packet against the routing table).

9. Huegen discloses routers have multi-paths, which packets can take to be routed (page 6, INFORMATION FOR VICTIMS AND HOW TO SUPPRESS ATTACKS, paragraphs 1-3). However, Huegen does not specifically disclose communicating the connection parameter differences to at least one other such intermediary device over an out-of-band communication channel. CERT discloses communicating the connection parameter differences to at least one other such intermediary device over an out-of-band communication channel (i.e., TCP/IP connection) (page 4, Alternative for routers that do not support filtering on the inbound side, paragraph 1). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Huegen and CERT because CERT's routing to alternative path would improve the throughput by dynamically switching the routing path to another one of possible routing paths to send the information.

10. As to claim 2, Huegen discloses synchronization module communicating a service request (i.e., TCP SYN) initially received from the requesting client to the at least one other such intermediary device while establishing the client-side connection over the out-of-band communications channel (i.e., TCP/IP connection) (page 9, OTHER DENIAL OF SERVICE ATTACKS WORTH OF MENTION, paragraphs 1 and 2). Furthermore, CERT discloses synchronization module communicating a service request (i.e., TCP SYN) initially received from the requesting client to the at least one other such intermediary device while establishing the client-side connection over the out-of-band communications channel (page 1, DESCRIPTION, paragraphs 1 and 2).

11. As to claim 3, Huegen discloses deferring communicating the connection parameter differences for transitory connections (page 2, HOW TO KEEP YOUR SITE FROM BEING THE SOURCE PERPETRATORS USE TO ATTACK VICTIMS, paragraph 4).

12. As to claim 4, Huegen discloses out-of-band communications channel comprises at least one of a broadcast (page 2, paragraph 1).

13. As to claim 5, Huegen discloses the connection-oriented network protocol is the Transmission Control Protocol (TCP) (page 9, OTHER DENIAL OF SERVICE ATTACKS WORTHY OF MENTION).

14. As to claim 6, Huegen discloses the intermediary device comprises at least one of a boundary controller (i.e., router; page 3, paragraph 1, i.e., IP version 4 routers, a router may have an option...). Huegen discloses filtering packets in order to defeat the possibility of source-address-spoofed packets from entering from downstream networks or leaving for upstream networks (page 2, HOW TO KEEP YOUR SITE FROM BEING THE SOURCE PERPETRATORS USE TO ATTACK VICTIMS, paragraph 2; page 6, last paragraph). However, Huegen does not specifically use a term firewall. CERT discloses a firewall (page 7, Fixes For IBM SNG Firewall). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Huegen and CERT because CERT's firewall would improve security of

Huegen's system by examining each messages and preventing unauthorized messages.

15. As to claim 8, it is rejected for the same reasons set forth in claim 2 above.

16. As to claim 9, it is rejected for the same reasons set forth in claim 3 above

17. As to claim 10, it is rejected for the same reasons set forth in claim 4 above.

18. As to claim 11, it is rejected for the same reasons set forth in claim 5 above.

19. Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Craig A. Huegen "The Latest in Denial of Service Attacks: "Smurfing" Description and Information to Minimize Effects", 2/8/2000, CERT Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks, Sep. 19, 1996 (Last Revised: Nov. 29, 2000), further in view of Schuba et al. (US 6,725,378), hereinafter Schuba.

20. As to claim 12, Huegen and CERT do not specifically disclose computer-readable storage medium holding code for performing the method of claim 7. However, Schuba discloses omputer-readable storage medium holding code (col. 7, lines 23-33; col. 11, line 67 – col. 12, line 14). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Huegen, CERT

and Schuba because Schuba's computer-readable storage medium would provide fast data storage and retrieval time.

21. Claims 13-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Craig A. Huegen "The Latest in Denial of Service Attacks: "Smurfing" Description and Information to Minimize Effects", 2/8/2000, in view of Moberg et al. (US 6,697,972), hereinafter Moberg.

22. As to claims 13 and 17, Huegen discloses the invention substantially as claimed, including a system for communicating routing information (i.e., routing table) between a plurality of link layer intermediary devices (i.e., routers, broadcast devices; page 2, HOW TO KEEP YOUR SITE FROM BEING THE SOURCE PERPETRATORS USE TO ATTACK VICTIMS, paragraph 6; page 6, INFORMATION FOR VICTIMS AND HOW TO SUPPRESS ATTACKS, paragraphs 3-6) in a network computing environment, comprising:

a link layer intermediary device (i.e., router, broadcast device) available from a plurality of link layer intermediary devices receiving a session packet from a requesting client (i.e., attacker) (page 1, DESCRIPTION, paragraph 1, lines 3-4; i.e., A perpetrator sends a large amount of ICMP echo traffic...);

generating an eco request packet identified as originating from the requesting client (i.e., filtering packets in order to defeat the possibility of source-address-spoofed packets from entering from downstream networks or leaving for upstream networks,

page 2, HOW TO KEEP YOUR SITE FROM BEING THE SOURCE PERPETRATORS USE TO ATTACK VICTIMS, paragraph 2; page 6, last paragraph) and addressed to a requested server (page 1, DESCRIPTION, paragraph 1, lines 5-6);

the link layer intermediary device forwarding the echo request packet to the requested server (i.e., deliver the echo request packet to the server; page 1, DESCRIPTION, paragraph 1, lines 5-7);

at least one other such link layer intermediary device receiving an echo response packet from the requested server (page 1, DESCRIPTION, lines 6-8; page 2, paragraph 1, lines 6-9);

the least one other such link layer intermediary device forwarding a response packet to the requested client (page 2, paragraph 1, lines 9-10).

23. Huegen does not specifically disclose encapsulating module and un-encapsulation module for un-encapsulating session packet. However, Moberg discloses encapsulating module (col. 5, lines 39-45; col. 6, lines 1-9 and 19-31) and un-encapsulation (i.e., decapsulation) module for un-encapsulating session packet (col. 5, lines 45-49 and 66-67; col. 6, lines 1-9 and 19-31). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Huegen and Moberg because Moberg's encapsulating and decapsulating would improve the reliability by allowing the packet to be properly routed to the intended destination.

24. As to claims 14 and 18, Huegen discloses echo request packet is an Internet Control Message Protocol (ICMP) echo request and the echo response packet is an ICMP echo response packet (page 1, DESCRIPTION, paragraph 1).

25. As to claims 15 and 19, Huegen discloses the connection-oriented network protocol is the Transmission Control Protocol (TCP) (page 9, OTHER DENIAL OF SERVICE ATTACKS WORTHY OF MENTION).

26. As to claim 16, Huegen discloses the intermediary device comprises at least one of a boundary controller (i.e., router; page 3, paragraph 1, i.e., IP version 4 routers, a router may have an option...). Huegen discloses filtering packets in order to defeat the possibility of source-address-spoofed packets from entering from downstream networks or leaving for upstream networks (page 2, HOW TO KEEP YOUR SITE FROM BEING THE SOURCE PERPETRATORS USE TO ATTACK VICTIMS, paragraph 2; page 6, last paragraph). However, Huegen does not specifically use a term firewall. CERT discloses a firewall (page 7, Fixes For IBM SNG Firewall). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Huegen and CERT because CERT's firewall would improve security of Huegen's system by examining each messages and preventing unauthorized messages.

27. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Craig A. Huegen "The Latest in Denial of Service Attacks: "Smurfing" Description and Information to Minimize Effects", 2/8/2000, Moberg et al. (US 6,697,972), further in view of Schuba et al. (US 6,725,378).

28. Huegen and Moberg do not specifically disclose computer-readable storage medium holding code for performing the method of claim 7. However, Schuba discloses omputer-readable storage medium holding code (col. 7, lines 23-33; col. 11, line 67 – col. 12, line 14). It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine the teachings of Huegen, Moberg and Schuba because Schuba's computer-readable storage medium would provide fast data storage and retrieval time.

Conclusion

29. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

Cox et al, patent 6,738,814, Yavatkar et al, patent 6,735,702, Todd, Sr. et al, patent 6,185,689, Coile et al, patent 6,298,380, Kirby et al, patent 5,828,846, Munger et al, patent 6,502,135, Bhaskaran, patent 5,963,540, Porras et al, patent 6,711,615, Magdych et al, patent 6,513,122 disclose method and system for checking a user is authorized to access a security vulnerabilities of a target host.

30. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jungwon Chang whose telephone number is (703)305-9669. The examiner can normally be reached on 9:30-6:00 (Monday-Friday).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John A Follansbee can be reached on (703)305-8498. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jungwon Chang
May 20, 2004

JOHN FOLLANSBEE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100